Original document

DATA ROBBERY PREVENTION DEVICE

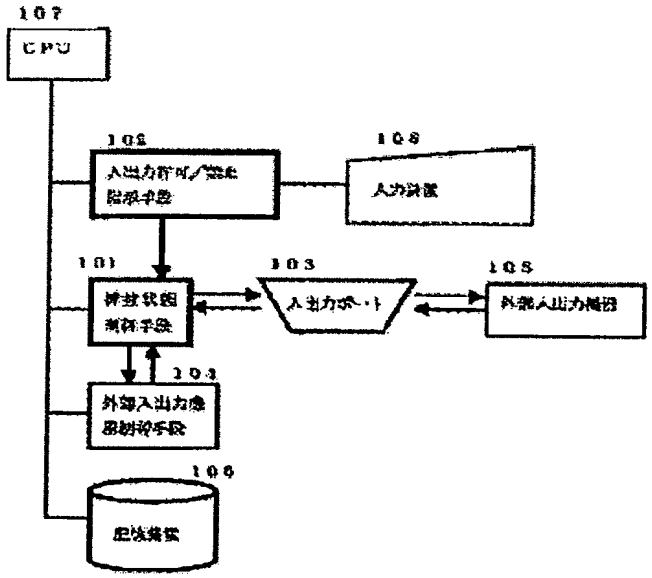
Publication number: JP2001154918
Publication date: 2001-06-08
Inventor: MATSUSHITA HISAFUMI
Applicant: MATSUSHITA ELECTRIC IND CO LTD
Classification:
- international: ***G06F13/14; G06F3/06; G06F12/14; G06F21/02; G06F21/24; H04L9/32;*** **G06F13/14; G06F3/06; G06F12/14; G06F21/00; H04L9/32;** (IPC1-7): G06F12/14; G06F3/06; G06F13/14; H04L9/32
- European:
Application number: JP19990337124 19991129
Priority number(s): JP19990337124 19991129

View INPADOC patent family
View list of citing documents

Report a data error here

Abstract of **JP2001154918**

PROBLEM TO BE SOLVED: To solve the problem that data are easily robbed by connecting an external storage device to an USB port or the like capable of live-line insertion and withdrawal even in an operation state. SOLUTION: The robbery of the data is easily prevented by an external input/output equipment control means for controlling the input/output of an external input/output equipment, an input/output permission/inhibition instruction means for instructing the permission/inhibition of the input/output and an insertion/withdrawal state control means for logically connecting/disconnecting the external input/output equipment corresponding to the permission/inhibition of data input/output.



Data supplied from the *esp@cenet* database - Worldwide

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2001－154918
（P2001－154918A）
(43)公開日　平成13年6月8日(2001.6.8)

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
G06F	12/14	320	G06F	12/14	320A　5B014
	3/06	301		3/06	301H　5B017
	13/14	330		13/14	330E　5B065
H04L	9/32		H04L	9/00	673A　5J104
					673D

審査請求　未請求　請求項の数9　OL　（全 5 頁）

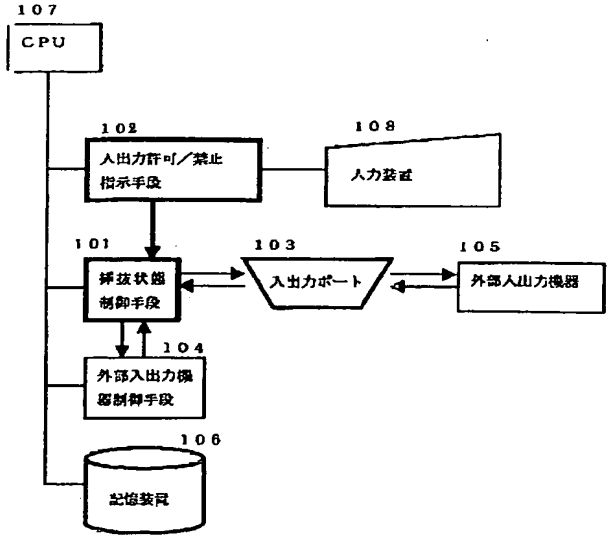
(21)出願番号　特願平11－337124
(22)出願日　平成11年11月29日(1999.11.29)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　松下　尚史
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100097445
弁理士　岩橋　文雄　（外２名）

Ｆターム(参考)　5B014 EA01 EB04 FA05 FB04 GD35 GE05 HC13
5B017 AA01 BA04 BA05 BA09 BB02 BB03 CA08 CA16
5B065 BA01 PA13 ZA03
5J104 AA07 KA01 NA27

(54)【発明の名称】　データ盗難防止装置

(57)【要約】
【課題】　動作状態でも活線挿抜可能なＵＳＢポート等に外部記憶装置を接続することでデータ盗難が容易に行われていた。
【解決手段】　外部入出力機器の入出力を制御する外部入出力機器制御手段と、入出力の許可／禁止を指示する入出力許可／禁止指示手段と、データ入出力の許可／禁止に応じて外部入出力機器を論理的に接続／未接続にする挿抜状態制御手段によってデータの盗難を容易に防止する。



【特許請求の範囲】
【請求項１】外部入出力機器の入出力を制御する外部入出力機器制御手段と、前記外部入出力機器に対する入出力の許可／禁止を指示する入出力許可／禁止指示手段と、前記入出力許可／禁止指示手段によって指示された前記外部入出力機器に対する入出力の許可／禁止に応じて前記外部入出力機器と前記外部入出力機器制御手段間の信号を接続／切断して前記外部入出力機器を接続状態／未接続状態にする挿抜状態制御手段とを有するデータ盗難防止装置。
【請求項２】正規のユーザーか否かを認証するユーザー認証手段を有し、前記ユーザー認証手段によって正規のユーザーと認証された場合にのみ入出力許可／禁止指示手段による外部入出力機器に対する入出力の許可／禁止の指示ができる請求項１記載のデータ盗難防止装置。
【請求項３】ユーザー入力が所定時間ないことを検知するユーザー入力監視手段を有し、前記ユーザー入力監視手段によってユーザー入力が所定時間ないことが検知された場合に入出力許可／禁止指示手段が外部入出力機器に対する入出力禁止を指示する請求項１ないし２記載のデータ盗難防止装置。
【請求項４】外部入出力機器の入出力を外部入出力制御手段によって制御する外部入出力機器制御手順と、前記外部入出力機器に対する入出力の許可／禁止を指示する入出力許可／禁止指示手順と、前記入出力許可／禁止指示手順で指示された前記外部入出力機器に対する入出力の許可／禁止に応じて前記外部入出力機器と前記外部入出力機器制御手段間の信号を接続／切断して前記外部入出力機器を接続状態／未接続状態にする挿抜状態制御手順から成るデータ盗難防止方法。
【請求項５】正規のユーザーか否かを認証するユーザー認証手順を含み、前記ユーザー認証手順によって正規のユーザーと認証された場合にのみ入出力許可／禁止指示手順で外部入出力機器に対する入出力の許可／禁止の指示がされる請求項４記載のデータ盗難防止方法。
【請求項６】ユーザー入力が所定時間ないことを検知するユーザー入力監視手順を含み、前記ユーザー入力監視手順でユーザー入力が所定時間ないことが検知された場合に入出力許可／禁止指示手順で外部入出力機器に対する入出力禁止が指示される請求項４ないし５記載のデータ盗難防止方法。
【請求項７】外部入出力機器の入出力を外部入出力制御手段によって制御する外部入出力機器制御ステップと、前記外部入出力機器に対する入出力の許可／禁止を指示する入出力許可／禁止指示ステップと、前記入出力許可／禁止指示ステップで指示された前記外部入出力機器に対する入出力の許可／禁止に応じて前記外部入出力機器と前記外部入出力機器制御手段間の信号を接続／切断して前記外部入出力機器を接続状態／未接続状態にする挿抜状態制御ステップから成るデータ盗難防止プログラムを記録した記録媒体。
【請求項８】正規のユーザーか否かを認証するユーザー認証ステップを含み、前記ユーザー認証ステップによって正規のユーザーと認証された場合にのみ入出力許可／禁止指示ステップで外部入出力機器に対する入出力の許可／禁止の指示がされる請求項７記載のデータ盗難防止プログラムを記録した記録媒体。
【請求項９】ユーザー入力が所定時間ないことを検知するユーザー入力監視ステップを含み、前記ユーザー入力監視ステップでユーザー入力が所定時間ないことが検知された場合に入出力許可／禁止指示ステップで外部入出力機器に対する入出力禁止が指示される請求項７ないし８記載のデータ盗難防止プログラムを記録した記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、外部入出力機器が接続できる入出力ポートを具備した情報処理装置におけるデータ盗難防止技術に関する。
【０００２】
【従来の技術】記憶メディアが着脱できるデータ記憶装置を有した従来の情報処理装置におけるデータ盗難防止対策として、例えば、フロッピーディスク・コントローラーをセットアップ・ユーティリティなどにより使用許可・禁止に設定できるようにしたものがある。使用禁止に設定した場合はフロッピーディスク・コントローラーはシステムに検出されないよう無効に設定され、結果的に内蔵フロッピーディスク装置そのものが使用できないようにしてデータ盗難を防止していた。
【０００３】
【発明が解決しようとする課題】しかしながら、近年の情報処理装置にはＵＳＢ機器やＰＣカードなどの外部の汎用入出力機器をシステムの稼動状態でも動的に接続できる活線挿抜可能な入出力ポートやスロットが設けられるようになり、ＵＳＢポートやＰＣカードを経由して外部記憶装置が接続可能になり、内蔵フロッピーディスク装置を使用禁止にしたところで必ずしもデータの盗難を防止することはできず、例えば、情報処理装置の電源を入れたまま席を離れた場合に、ＵＳＢフロッピー装置やメモリーカードやＡＴＡカードが他人に挿入されると簡単にデータが盗難されてしまっていた。
【０００４】また、従来の内蔵フロッピーディスク装置の使用禁止はセットアップユーティリティなどを用いて行っていたため、システムの稼働中には使用禁止・許可を動的に切り替えることができず、正規ユーザーが内蔵フロッピーディスク装置を使用したい場合にはシステムを再起動して使用禁止・許可を設定する必要があり操作性が悪かった。
【０００５】本発明は、汎用的な外部入出力機器がシステムの稼動状態でも動的に接続可能な情報処理装置にお

いて、データの盗難を防止することを目的とする。

【0006】

【課題を解決するための手段】上記課題を解決するために本発明は、外部入出力機器の入出力を制御する外部入出力機器制御手段と、外部入出力機器に対する入出力の許可／禁止を指示する入出力許可／禁止指示手段と、入出力許可／禁止指示手段によって指示された外部入出力機器に対するデータ入出力の許可／禁止に応じて外部入出力機器と外部入出力機器制御手段間の信号を接続／切断して外部入出力機器を接続状態／未接続状態にする挿抜状態制御手段を有することで、ユーザーが簡単に外部入出力機器に対する入出力禁止を指示でき、データ盗難を防止することができる。

【0007】また、正規のユーザーか否かを認証するユーザー認証手段を有し、ユーザー認証手段によって正規のユーザーと認証された場合にのみ入出力許可／禁止指示手段による外部入出力機器に対する入出力の許可／禁止の指示ができるようにすることで、特定ユーザーのみが外部入出力機器に対する入出力を行えるようになり、セキュリティレベルを向上することができる。

【0008】また、ユーザー入力が所定時間ないことを検知するユーザー入力監視手段を有し、ユーザー入力監視手段によってユーザー入力が所定時間ないことが検知された場合に入出力許可／禁止指示手段が外部入出力機器に対する入出力禁止を指示するようにすることで、入出力の禁止指示を忘れて席を離れた場合にも自動的に外部入出力機器に対する入出力が禁止され、セキュリティレベルをさらに向上することができる。

【0009】

【発明の実施の形態】以下、本発明の実施の形態について、図1、図2を用いて説明する。

【0010】（実施の形態1）図1は本実施の形態に係るデータ盗難防止装置の構成図である。

【0011】図1において、105はフロッピーディスク装置等の外部入出力機器、103は外部入出力機器105が接続される入出力ポート、104は外部入出力機器105の入出力を制御する外部入出力機器制御手段、106はデータが格納されている記憶装置、108はユーザーがデータ等を入力する入力装置、101は外部入出力機器制御手段104に対して外部入出力機器105の論理的な挿抜状態の制御を行う挿抜状態制御手段、102は入力装置108からのユーザーの指示によって外部入出力機器105の入出力の許可／禁止を指示する入出力許可／禁止指示手段、107はシステム全体の制御を行うCPUである。

【0012】これにより、データ入出力禁止の場合には外部入出力機器105の物理的な挿抜に関わらず論理的に未接続状態となって外部入出力機器105は使用不可能となり、記憶装置106からの不正なデータ盗難を防止することができる。

【0013】また、入出力許可／禁止指示手段102によってシステムを再起動することなく外部入出力機器105の入出力の許可／禁止指示ができる。

【0014】（実施の形態2）図2は本実施の形態に係るデータ盗難防止装置の構成図である。

【0015】図2において、109は入出力の許可／禁止指示ができるユーザーか否かを認証するユーザー認証手段、110は入力装置108からのユーザー入力の有無を監視するユーザー入力監視手段であって、他の構成要素は実施の形態1に示されたものと同じである。

【0016】ユーザー認証手段109は、例えば、パスワードや指紋など特定のユーザーを認証する手段であり、ここでの認証に合格した場合にのみ入出力許可／禁止指示手段102によって外部入出力機器105に対する入出力の許可／禁止指示を与えることができる。

【0017】ユーザー入力監視手段110は、入力装置108からの入力状態を監視してユーザーからの入力が一定時間ない場合には入出力許可／禁止指示手段102によって外部入出力機器105に対する入出力の禁止指示を出す。これによって、ユーザーが入出力禁止指示を忘れた場合でも、一定時間入力がなければ自動的に外部入出力機器105の使用が禁止される。

【0018】

【発明の効果】以上詳述したように、本発明によれば物理的に外部入出力機器を挿抜することなく論理的に接続／未接続状態にできることで外部入出力機器を使ったデータの盗難を容易に防止することができる。

【0019】また、入出力ポートを介してデータ盗難防止装置から電源を確保している外部入出力機器の場合には論理的に未接続状態にすれば電源供給も停止され、省電力にも効果がある。

【図面の簡単な説明】

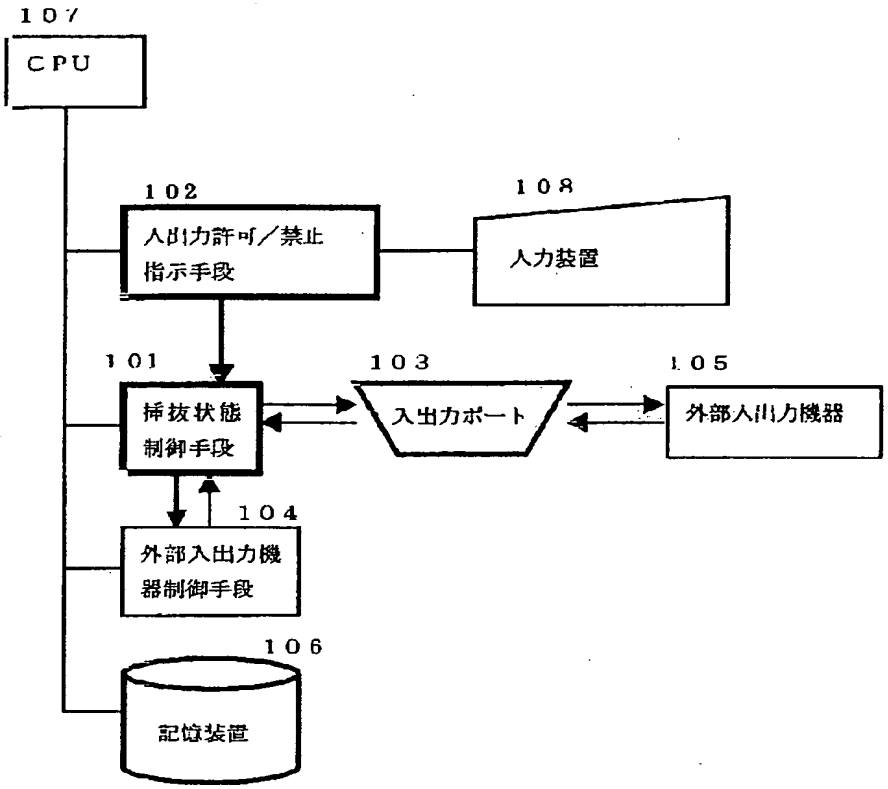
【図1】本発明の実施の形態1に係るデータ盗難防止装置の構成図

【図2】本発明の実施の形態2に係るデータ盗難防止装置の構成図

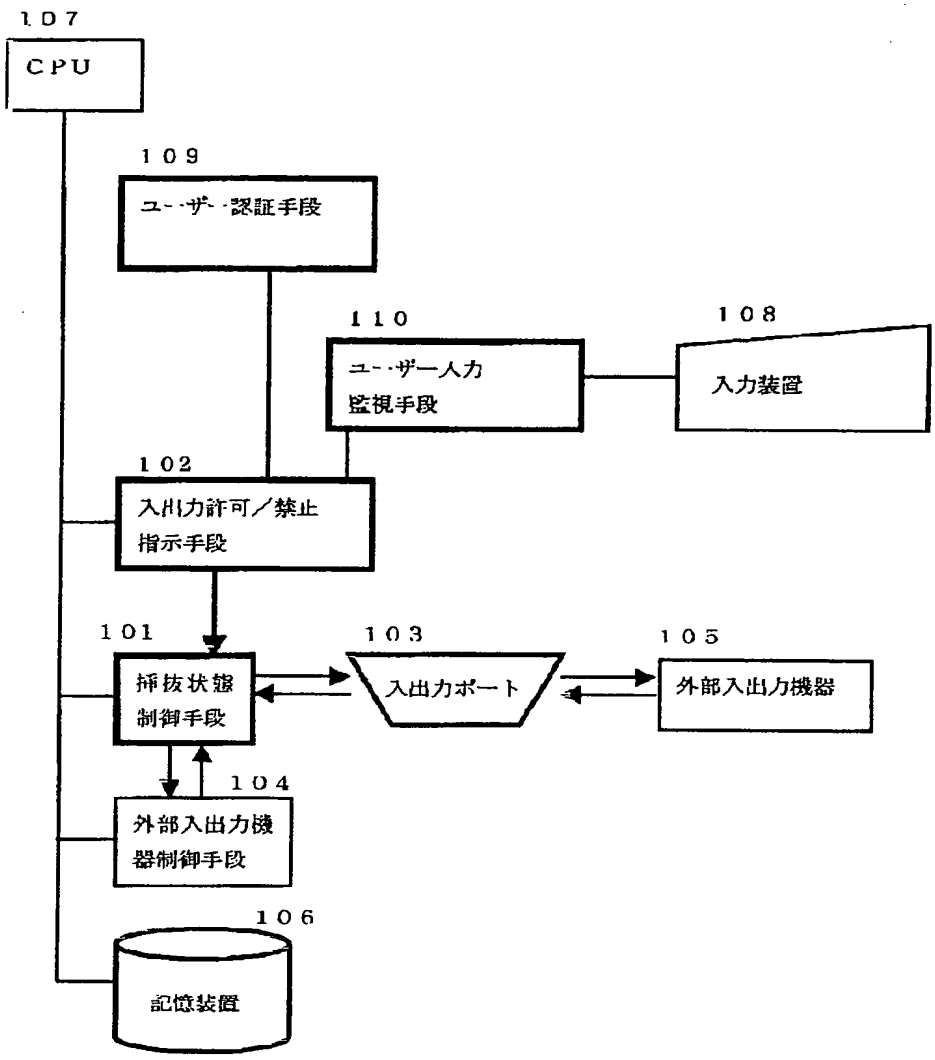
【符号の説明】

101　挿抜状態制御手段
102　入出力許可／禁止指示手段
103　入出力ポート
104　外部入出力機器制御手段
105　外部入出力機器
106　記憶装置
107　CPU
108　入力装置
109　ユーザー認証手段
110　ユーザー入力監視手段

【図1】


107
CPU
102
入出力許可／禁止
指示手段
108
入力装置
101
挿抜状態
制御手段
103
入出力ポート
105
外部入出力機器
104
外部入出力機
器制御手段
106
記憶装置

【図2】


107
CPU
109
ユーザー認証手段
110
ユーザー入力
監視手段
108
入力装置
102
入出力許可／禁止
指示手段
101
挿抜状態
制御手段
103
入出力ポート
105
外部入出力機器
104
外部入出力機
器制御手段
106
記憶装置